

What is claimed is

1. A method of re-configuring a network element of a transmission network to restore traffic after a failure, said method comprising the steps of:
 - generating a configuration request to implement a new cross-connection through said network element,
 - performing said request in a first fetch-ahead phase comprising only configuration steps essential for fast implementation of said cross-connection and skipping security related configuration steps thereby providing reduced security against process restarts; and
 - performing said request in a second consolidation phase comprising said previously skipped security related configuration steps.
2. A method according to claim 1, wherein said consolidation phase comprises a consistency check of said request and storing of the configuration changes in a persistent local database.
3. A method according to claim 1, wherein execution of said request in the fetch-ahead phase leads to an inconsistency between actual hardware configuration and locally stored configuration data of said network element and wherein during said consolidation phase, said inconsistency is resolved.
4. A method according to claim 1, wherein a timer is started during said fetch-ahead phase and if said timer lapses before said consolidation phase has

been completed, configuration steps performed during fetch-ahead are undone by re-loading stored configuration data.

5. A network element of a transport network, comprising a number of input and output ports, a crossconnection matrix for randomly establishing connections from any to an port and at least one controller for configuring said network element and establishing crossconnections through said matrix; said controller being adapted to perform a received configuration request in a fetch-ahead phase first and to perform said request in a consolidation phase thereafter; wherein said fetch-ahead phase comprises only configuration steps essential for fast implementation of said cross-connection and skipping security related configuration steps thereby providing reduced security against process restarts; and wherein said consolidation request comprises said previously skipped security related configuration steps.

6. A network element according to claim 5, wherein said controller comprises a layered control software with at least two software layers, a first software layer comprising an abstraction of physical and logical resources of said network element for the purpose of network management and a second software layer comprises a representation of the actual hardware modules of the network element and its configuration, each of said software layers comprising a individual persistent storage storing an image of configuration data of the corresponding software layer; said controller being adapted to successively process said request in each of said layers and forward it to the next lower layer, wherein storing of configuration data to the persistent storage is performed in each of said layers during consolidation phase, only.

7. A network element according to claim 5, wherein said consolidation phase comprises a consistency check of said request and storing of the configuration changes in a persistent local database.

8. A network element according to claim 5, wherein execution of said request in the fetch-ahead phase leads to an inconsistency between actual hardware

configuration and locally stored configuration data of said network element and wherein during said consolidation phase, said inconsistency is resolved.

9. A network element according to claim 5, further comprising a timer which is started during said fetch-ahead phase and if said timer lapses before said consolidation phase has been completed, configuration steps performed during fetch-ahead are undone by re-loading stored configuration data.